

## **AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANT**

I, Special Agent Beach, having been duly sworn on oath, state as follows:

### **Affiant's Background**

1. I am a Special Agent with the Department of Homeland Security, currently assigned to the Arizona office of Homeland Security Investigations (HSI) and have been since 2015. I was previously a Border Patrol Agent with the United States Border Patrol for eleven years. I am a graduate of the Criminal Investigator Training Program conducted by the Federal Law Enforcement Training Center, Glynco, GA. During my career in law enforcement, I have participated in multiple investigations involving illegal drugs, cybercrimes, the darknet, and numerous search warrants.

2. I have participated in the execution of search and seizure warrants involving electronic evidence and have been involved in investigations of narcotics-related crimes. I have conducted investigations concerning the unlawful distribution of illegal narcotics, possession with intent to distribute controlled substances, importation of illegal narcotics, use of communications to conduct illegal narcotics transactions, maintaining places for purposes of manufacturing, distributing, or using controlled substances, and conspiracies to commit these offenses, in violation of Title 21, United States Code, Sections 841, 843, 846, 952, and 963. Based upon this experience, and conversations with other investigators and detectives with numerous years of experience, I have also become well-versed in the methodology utilized in illegal narcotics trafficking, the specific type of language used by illegal narcotics traffickers, and the unique patterns employed by narcotics organizations. I have also conducted physical surveillances and electronic surveillances. Additionally, I

have arrested individuals for various drug violations and have spoken with several drug dealers, drug users, and informants concerning the methods and practices of drug traffickers.

3. I have had many discussions with other experienced law enforcement officers and have conducted, and been present at, many interviews of self-admitted narcotics traffickers and cooperating defendants concerning how drug traffickers and money launderers operate. I know that drug traffickers often hold proceeds traceable to their drug-trafficking activities in the form of United States currency, funds in bank accounts, high-value personal property items, and real property. But I also know that drug traffickers are now increasingly holding drug-trafficking proceeds in virtual currency or cryptocurrency.

4. Based on my training, research, education, and experience, I am familiar with the relevant terms and definitions set forth in the section titled “Background on the Darknet and Cryptocurrency” below. I know that cryptocurrencies are different from traditional currencies in that cryptocurrencies are not issued by or backed by any government. In addition, cryptocurrency accounts and wallets are different from traditional bank accounts in that these accounts are held in digital format in one of any number of various types of digital wallets or exchanges. Likewise, cryptocurrency is accessible only by the account holder or someone who has access to the account password or account “recovery seed<sup>1</sup>,” a

---

<sup>1</sup> A “recovery seed” is a mnemonic passphrase made up of 12 random words. It acts as a backup, ensuring that the wallet’s funds can always be accessed. Anyone with the “recovery seed” can gain access to and control the wallet’s funds. The recovery seed is a root key, sometimes referred to as a root seed, recovery seed, or mnemonic seed. A root key is a back-up key to the private key and allows a wallet owner to re-generate a new key pair for the corresponding wallet, offline and outside of the company or software that originally generated it. After re-generating

mnemonic passphrase made up of a series of random words, or in some circumstances, by the company hosting the virtual wallet containing the cryptocurrency. Account holders have the ability to send and receive cryptocurrency using a unique and complex wallet address, often referred to as the private key.

5. Because I am submitting this affidavit for the limited purpose of establishing probable cause for the requested seizure warrants, I have not included in this affidavit every detail I know about this investigation. Rather, I have included only the information necessary to establish probable cause for the requested seizure warrants.

6. The facts set forth in this affidavit are based on my personal knowledge, including what I have learned through my training and experience as a law enforcement officer, my review of documents and other records obtained in the course of this investigation, and information I have obtained in the course of this investigation from witnesses having personal knowledge of the events and circumstances described herein and other law enforcement officers, all of whom I believe to be truthful and reliable.

### **Introduction**

7. I submit this affidavit in support of applications for a warrant to seize the following vehicle controlled by Javier VILLASENOR, which is specifically described as follows:

a. 2014 Nissan GTR 2 door coupe – Vehicle identification Number (VIN)

JN1AR5EF4EM270940

---

the wallet with a root key, the possessor of the new wallet now has the ability to send and receive the value (in this example, cryptocurrency) associated with the original key pairs using the new private key created by the root key or “recovery seed.”

(Hereinafter referred to as the “Subject Vehicle”).

8. For the reasons set forth below, I submit that there is probable cause to believe that the Subject Vehicle constitutes or is derived from proceeds traceable to mail fraud, in violation of 18 U.S.C. § 1341, and was involved in the commission of money laundering offenses, in violation of 18 U.S.C. §§ 1956 and 1957, and therefore is:

- a. Subject to civil forfeiture under 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C);
- b. Subject to criminal forfeiture under 18 U.S.C. §§ 981(a)(1)(C), 982(a)(1), and 28 U.S.C. § 2461; and
- c. Subject to seizure via a civil seizure warrant under 18 U.S.C. § 981(b) and 21 U.S.C. § 881(b) and via a criminal seizure warrant under 21 U.S.C. § 853(f).

### **Background on the Darknet and Cryptocurrency**

9. The “darknet” is a portion of the “Deep Web” of the internet,<sup>2</sup> where individuals must use anonymizing software or an application to access content and websites. The darknet is home to criminal marketplaces, also called “hidden services”, where individuals can buy and sell illegal items, such as drugs, firearms, and other hazardous materials with greater anonymity than is possible on the traditional internet (sometimes called the “clear web” or simply the “web”). Darknet Marketplaces (DNMs) operate in a manner similar to clear-web commercial websites, such as Amazon and eBay, but they offer illegal items and

---

<sup>2</sup> The Deep Web is the portion of the internet not indexed by search engines. Examples are databases and internal networks belonging to private industry, government agencies, or academic institutions.

they also use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to shield communications and transactions from interception and monitoring. Examples of such DNMs that offered illicit goods and services include Silk Road, AlphaBay, and Hansa, all of which have since been shut down by law enforcement.

10. On DNMs, vendors create and operate “vendor accounts” and customers create and use “customer accounts,” just as legitimate vendors and customers do on clear-web marketplaces. Vendor and customer accounts are not identified by numbers, but rather monikers or “handles,” much like the username one would use on a legitimate clear website. If a moniker on a particular marketplace has not already been registered by another user, vendors and customers can use the same moniker across multiple marketplaces, and based on seller and customer reviews, can become well known as “trusted” vendors or customers. It is also possible for the same person to operate multiple customer accounts and multiple vendor accounts at the same time. For example, based on my training and experience, I know that one person could have a vendor account that he or she uses to sell illegal goods on a DNM in exchange for cryptocurrency, while that same vendor could also have a different customer account that he or she uses to exchange cryptocurrency earned from vendor sales for fiat currency.<sup>3</sup> Likewise, a person on the darknet could use different accounts to send and receive the same cryptocurrency. I know from training and experience that one of the reasons DNM vendors often have and use

---

<sup>3</sup> Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

multiple vendor and customer accounts is to conceal from law enforcement both their identities and which accounts they own and control.

11. The “Tor network,” or simply “Tor” (an abbreviation for “The Onion Router”), is a special network of computers on the internet, distributed around the world, whose purpose is to conceal the true Internet Protocol (“IP”) addresses of the computers accessing the network, and, thereby, the locations and identities of the network’s users. Tor also enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as “hidden services” on the Tor network. Such hidden services operating on Tor have complex web addresses, generated by a computer algorithm, ending in “.onion” and can only be accessed through specific web browser software, including a browser known as “Tor Browser,” designed to access the Tor network. Examples of hidden services websites are AlphaBay and Hansa. Tor is available on cellphones using the Android and Apple operating systems by installing an application that puts a Tor enabled internet browser on a user’s cellphone, which then routes the phone’s IP address through different servers all over the world, making it extremely difficult to track.

12. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether.

13. Cryptocurrency can exist digitally on the internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public

and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object.

14. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries.

15. Generally, cryptocurrency is not issued by any government, bank, or company. Instead, cryptocurrency is generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.<sup>4</sup> Cryptocurrency is not illegal in the United States.

16. Bitcoin<sup>5</sup> (“BTC”) is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (*i.e.*, online companies that allow individuals to buy or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by “mining.” An individual can “mine” bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals

---

<sup>4</sup> But some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

<sup>5</sup> Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter “B”) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter “b”) to label units of the cryptocurrency. That practice is adopted here.

are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as “pseudonymous,” meaning that they are partially anonymous. And although bitcoin transactions are not completely anonymous, bitcoin does allow users to transfer funds more anonymously than traditional financial transactions.

17. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and then generate, store, or generate and store public and private keys used to send and receive cryptocurrency. A public key, or public address, is akin to a bank account number. A private key, or private address, is akin to a PIN number or password that allows a user to access and transfer value associated with the public address or key.

18. To conduct transactions on a blockchain, an individual must use the public address as well as the private key. A public address is represented as a case-sensitive string of letters and numbers, 26–35 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of a



public address's private key can authorize any transfers of cryptocurrency from that cryptocurrency public address to another cryptocurrency address.

19. Each private key and/or wallet can control multiple public addresses. These groupings of public addresses associated with one private key or wallet are referred to as address clusters. These linked addresses can be identified by investigators through co-spend and change transactions shown on the blockchain. A co-spend is a transaction in which two or more blockchain addresses send a balance to an additional blockchain address, which indicates that the multiple sending addresses are associated with the same wallet or private key. A co-spend is a transaction in which two or more blockchain addresses send a balance to an additional blockchain address, which indicates that the multiple sending addresses are associated with the same wallet or private key. A change address is a blockchain address that receives the remainder of cryptocurrency sent to an additional address in a transaction. As the Bitcoin cryptocurrency protocol necessitates sending an address' entire balance in any transaction, the amount not intended to be deposited is returned to the sender as change. These change addresses can be attributed to the sender's private key or wallet.

20. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is frequently used by individuals and organizations for criminal purposes, such as to pay for illegal goods and services – via, for example, hidden services websites operating on the Tor network.

21. Cryptocurrencies can also be used to engage in money laundering. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the DNMs.

22. A cryptocurrency user can store and access wallet software in a variety of forms, including via:

- a) a PC or laptop ("desktop wallet"),
- b) a mobile application on a smartphone or tablet ("mobile wallet"),
- c) an internet-based cloud storage provider ("online wallet"),
- d) an online account associated with a cryptocurrency exchange ("online account"),
- e) a tangible, external device, such as a USB thumb drive ("hardware wallet"), or
- f) printed public and private keys ("paper wallet").

Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (*e.g.*, smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (*e.g.*, Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code<sup>6</sup> with the public and private key embedded in the code. Paper wallet keys are not stored digitally.

---

<sup>6</sup> A QR code is a matrix barcode that is a machine-readable optical label.

23. Wallets can also be backed up via, for example, paper printouts, USB drives, or CDs. Wallets can be accessed through a password or a “recovery seed” or “mnemonic phrase,” that is, random words strung together in a phrase.

24. Additional security safeguards for cryptocurrency wallets can include two-factor authorization, such as a password and a phrase. I know that individuals possessing cryptocurrencies often have safeguards in place to prevent their assets from hacking, unauthorized transfer, and/or law enforcement seizure.

25. Cryptocurrency “exchangers” and “exchanges” are individuals or companies that exchange or transmit bitcoin and other cryptocurrencies for other currencies, including U.S. dollars. According to Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) Guidance issued on March 18, 2013, and May 9, 2019, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses (“MSBs”).<sup>7</sup> MSBs, including cryptocurrency exchanges, function as regulated businesses subject to the federal Bank Secrecy Act (“BSA”).<sup>8</sup> Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering (AML) regulations, “Know Your Customer” (KYC) protocols, and other verification procedures similar to those employed by traditional

---

<sup>7</sup> See FinCEN Guidance FIN-2019-G001, “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies,” May 9, 2019; FinCEN Guidance FIN-2013-G001, “Application of FinCEN’s Regulations to Person Administering, Exchanging, or Using Virtual Currencies,” March 18, 2013.

<sup>8</sup> Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1118 (1970).

financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% of the amount exchanged, in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%.

26. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application. But many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed, or on any digital or physical backup private key that the user creates. As a result, these wallet service companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet

application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet, described above, law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and then transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

27. As of May 6, 2022, one bitcoin is worth approximately \$35,980 U.S. Dollars (USD). But the value of bitcoin is volatile, and its value, to date, has been more volatile than that of widely accepted fiat currencies such as the U.S. Dollar.

#### **Facts Supporting Findings of Probable Cause**

28. On August 3, 2021, Homeland Security Investigations (HSI) Tucson received information from a Postal Inspector with the United States Postal Inspection Service (USPIS) in Tucson, AZ regarding several parcels that had been mailed with suspicious characteristics.

29. Namely, they were mailed from Tucson, Arizona which is an area known to be a source area for narcotics that are often shipped across the country. The parcels had tracking numbers, but no phone numbers associated with the parcels. From my experience, I know that nearly all drug and drug sales proceeds parcels bear tracking numbers allowing the sender and receiver to track the progress of the shipment from origination to destination. There were no telephone numbers listed on the mailing label for either the sender or addressee. In my experience, legitimate mailers who use the United States Postal Service (USPS) Priority Mail service regularly include telephone numbers in the spaces provided on the label because they paid a premium price for the service and want to be contacted to

help facilitate a timely delivery should a problem arise. In my experience, Priority Mail parcels that I have seized drugs and/or drug proceeds from bore either no telephone numbers or listed fictitious telephone numbers.

30. Through various USPS and law enforcement databases, investigators were also able to associate the mailer of the suspect parcels to a previously mailed parcel that was discovered to contain misbranded and counterfeit drugs that looked like generic Xanax tablets (similar shape, coloring, and contained the imprints of generic manufacturers of the drug) containing the controlled substance Alprazolam but in fact when lab tested contained either Clonazepam or Bromazepam. Clonazepam and Bromazepam have not been approved for medical purposes by the FDA.

31. On August 4, 2021, USPIS Postal Inspectors conducted a positive canine sniff on four of the suspicious parcels identified on August 3, 2021, and then applied for a federal search warrant to further examine the parcels. The Inspectors were granted the search warrant (21-05911MB) and seized a total of 2,047.66 grams of what looked like manufactured generic Xanax tablets but when lab tested contained Clonazepam. All four of these parcels used the same fake return address name of CHAMBRUN and the same Tucson residential return address. No company or person using anything like CHAMBRUN was found connected to the address.

32. Investigators analyzed characteristics in common with these parcels and established a pattern to target. Investigators began to conduct surveillance at the main Tucson Post Office during the time of day that most of these parcels had been shipped.

33. Investigators also examined security camera footage from the main Tucson Post Office and observed a subject that they believed shipped the four parcels seized on August 4, 2021. Investigators were later able to identify this subject as Jose QUIROZ.

34. On August 9, 2021, during surveillance operations at the main Tucson Post Office, investigators observed QUIROZ arrive, withdraw a USPS plastic carrier bin full of USPS parcels out of the trunk of a vehicle, carry them into the main Tucson Post Office and set the parcels on the counter to be scanned into USPS systems for delivery.

35. Investigators then observed QUIROZ drive to the Tucson Coronado Post Office and repeat his delivery pattern there. QUIROZ removed more USPS parcels from the vehicle, carried them into the Coronado Post Office and left them there for delivery.

36. Investigators then observed QUIROZ drive to a warehouse located at 4334 East Illinois Street, Tucson, AZ 85714. Investigators saw QUIROZ leave the warehouse a short time later and followed QUIROZ again back to the Coronado Post Office. Investigators then witnessed QUIROZ deliver more parcels inside to USPS. QUIROZ then returned to the warehouse location, got into a different vehicle, and left.

37. A short time later, investigators observed the first vehicle leave the warehouse location with a different driver who was later identified as Javier A. VILLASENOR Medina. Investigators followed VILLASENOR driving the vehicle to his Tucson, AZ residence.

38. On August 31, 2021, at approximately 1600 hours, investigators were conducting further surveillance when they observed VILLASENOR leave his residence and drive to the warehouse location on Illinois Street. They observed VILLASENOR exit

the warehouse at approximately 1630 hours with USPS plastic carrier bins full of USPS parcels and place them into the trunk of a vehicle. VILLASENOR then drove to the Tucson Mission Post Office and carry in several larger USPS parcels for delivery. VILLASENOR was photographed during these activities and returned to the vehicle empty handed.

39. VILLASENOR then drove to the Main Tucson Post Office and investigators watched him take a USPS plastic carrier bin full of USPS parcels and walk inside. VILLASENOR returned with the empty carrier bin, placed it in the back seat of the vehicle and then walked back into the Tucson Main Post Office with another plastic carrier bin full of USPS parcels. At this time surveillance was terminated.

40. On August 31, 2021, USPIS Inspectors intercepted one of the parcels observed delivered by VILLASENOR at the Tucson Mission Post Office. USPIS Inspector's opened this parcel pursuant to federal search warrant (21-03200MB) and it contained similar looking pills as the other seizures (they looked like otherwise legitimate generic Xanax tablets) which when lab tested turned out to contain Clonazepam and not Alprazolam which is the active ingredient in Xanax. The weight of the pills was 1,175 grams.

41. On September 7, 2021, at approximately 2:50 p.m., a USPIS Inspector observed VILLASENOR's vehicle exiting the Tucson Main Post Office parking lot. He went inside the lobby and saw seven parcels with BBB Club as the return address business name. Investigators have seen the BBB Club name before listed by VILLASENOR on parcels in the past and have not been able to identify it as a real business or establishment. The use of fake or fictitious return sender names and addresses is one of the patterns noted



by investigators for VILLASENOR's mailing methods. The USPIIS Inspector was able to observe VILLASENOR on security camera recordings delivering these above-mentioned parcels on September 7, 2021.

42. On September 25, 2021, law enforcement in Barbourville, Kentucky executed a search warrant at a suspect's residence and discovered more than 179 grams of blue rectangular pills marked "B707" and yellow rectangular pills marked "R039". These are the exact types of pills VILLASENOR has shipped in the past and appeared to be the same as the ones previously seized from VILLASENOR shipments. The suspect stated he had been purchasing these "Xanax" pills from a dark web vendor named HULKSMACK for approximately 6 to 12 months and would make purchases at least once a week. US Postal records showed that at least 11 parcels from Tucson had been shipped to this same Kentucky residence since March 2021. All 11 of these parcels used fake sender companies and addresses in Tucson that either had been used by VILLASENOR before or fit the same pattern of fake company name paired with a seemingly random residential address.

43. Screen shots from this suspect's computer show some of his order history from the White House Market, which included an order for "1000X R039 Xanax 2.5MG" from HULKSMACK. It also shows an order for "500X B707 Xanax 2.5MG" from HULKSMACK. It is clear that VILLASENOR shipped parcels from the HULKSMACK moniker which was advertising these pills as either B707 Xanax or R039 Xanax. The suspect believed he was purchasing pills from VILLASENOR that contained "Xanax" or alprazolam which is a Schedule IV controlled substance. Lab results clearly indicate that

the pills, despite their appearance and advertising otherwise, contained either Clonazepam or Bromazepam.

44. Legitimate yellow “R039” rectangle pills are manufactured by Actavis and are in fact generic Alprazolam pills which is the active ingredient for Xanax. Legitimate “B707” rectangle pills are manufactured by Breckenridge Pharmaceutical Inc. and are also generic Alprazolam pills.

45. Completed lab results from each of the parcels throughout the entirety of this investigation contained what appeared to be generic Xanax pills but were in fact either Clonazepam or Bromazepam. Despite being shaped, imprinted and colored to be Xanax or its generic equivalent, the active ingredient for Xanax and its generic versions, alprazolam, was not present in any of these parceled pills distributed or attempted to be distributed by VILLASENOR through the U.S. mail.

46. After analyzing more complete USFIS data, investigators determined that the VILLASENOR darknet Drug Trafficking Organization (DTO):

- a. Sent approximately 2,400 parcels between January 2021 and January of 2022.
- b. Shipped more than 1,500 kilograms of illicit pills (the seven parcels seized in this case so far, have yielded an average of 648 grams per parcel)
- c. Paid over \$18,000 USD worth of cryptocurrency for prepaid USPS postage labels.

47. Following the identification of QUIROZ delivering parcels to the post office, Javier VILLASENOR was identified as an associate of QUIROZ. Using CBP databases, a

shipment of ledger USB devices was determined to have been delivered to VILLASENOR at his 3065 Fontana Ave. residence in Tucson, AZ in October of 2019. A ledger USB is a type of cold-storage wallet. These devices are indicative of cryptocurrency use and knowledge at a level above that of the average user, indicating that VILLASENOR has this advanced crypto currency knowledge. The knowledge that he likely possessed these devices is what led to the initial issuance of subpoenas to Coinbase and other cryptocurrency exchanges based on VILLASENOR's personally identifying information.

48. The cryptocurrency exchange accounts described in paragraph 7 received incoming deposits from blockchain addresses associated with addresses identified as blockchain addresses used for outgoing deposits by DNM vendors, as determined by previous investigations and tracing efforts. The value and volume of the cryptocurrency deposited into VILLASENOR's cryptocurrency exchange accounts significantly increased in 2021, despite reporting no employment income since 2019. Since his last reported employment, VILLASENOR received cryptocurrency deposits equivalent to approximately \$20,856 USD in 2020 and approximately \$555,566 USD in 2021. The specific accounts or wallets seen on the documents with articulable account identification data, and details on the activity associated with each account is outlined as follows:

a. Coinbase –

- i. Coinbase is a United States based cryptocurrency exchange company. Users of this service commonly deposit U.S. fiat currency to be converted or traded via send/receive functions within the account application.

- ii. Investigators learned that VILLASENOR opened a Coinbase account in December 2017 and served them with a subpoena. Per the blockchain tracing of transaction activity documented in the subpoena returns from Coinbase, VILLASENOR frequently sent cryptocurrency to an address cluster attributed to Bitcoinz.io. Bitcoinz.io provides services for purchases made via bitcoin (BTC), as opposed to fiat currency. Notably, bitcoinz.io is a service attributed to the use of BTC to purchase prepaid USPS postage labels. This is a common tactic of criminals shipping drugs through the USPS since it provides some anonymity.
- iii. Seventeen deposits into VILLASENOR's Coinbase account received between April 29, 2020 and August 4, 2021, worth 1.5885 BTC, were determined through tracing conducted by investigators to have sent from addresses associated with illicit DNM activity.
- iv. Between June 22, 2019, and August 4, 2021, cryptocurrency equivalent to \$19,874 USD deposited into this account was sold and withdrawn into banking accounts controlled by VILLASENOR.

b. Binance –

- i. Binance is a cryptocurrency exchange company currently based in the Cayman Islands. Users of this service commonly deposit fiat currency to be converted or traded via send/receive functions within the account application. United States citizens cannot currently open or maintain a Binance exchange account.
- ii. Investigators identified a Binance cryptocurrency account controlled by VILLASENOR that appears to have been opened using someone else's identification, or a "synthetic ID". These types of "synthetic IDs" can be found for sale on various DNMs and not only include a fake ID document but selfie pictures and digital Personally Identifiable Information (PII) often needed to pass cryptocurrency exchanges KYC requirements encountered when opening new accounts. Investigators learned of this Binance account from a deposit in to VILLASENOR's Coinbase account in February 2021.
- iii. Records provided by Binance pursuant to a subpoena demonstrate that this account was opened using a photograph matching an identity document for a "Shawn B Hunter" from Ontario, Canada. Other records from Binance list an email address and phone number known to belong to VILLASENOR. Device IDs and names captured in the Binance account's IP access logs show that an iPhone 13 with

a device ID name (set by the iPhone owner or operator) of “Javier VILLASENOR’s iPhone” accessed the Binance account and initiated transactions on many occasions. These IP access logs captured mostly Virtual Private Network (VPN) IP addresses accessing the account. Investigators have learned that criminals often use VPNs to prevent logging their true home IP address.

- iv. While reviewing IP logs provided by this cryptocurrency exchange, investigators observed IP address 174.18.1.17. Per the American Registry for Internet Numbers (ARIN), IP address 174.18.1.17 is registered to internet provider CenturyLink Communications, LLC, in Tucson, Arizona. A subpoena requesting subscriber information for this IP address was sent to CenturyLink Communications and the records they returned pursuant to the subpoena showed that this IP address returned to VILLASENOR’s home address. This IP address is also present in the IP address logs returned by Coinbase. That Coinbase account was opened using VILLASENOR’s Arizona Driver’s License. This IP Address and Device ID information indicates that VILLASENOR is the owner of this cryptocurrency account that was opened with the Canadian identity documents belonging to “Shawn B Hunter”.

- v. Investigators also learned from these financial records that VILLASENOR has transferred some of his cryptocurrency in and out of online gambling sites that accept cryptocurrency. Many online cryptocurrency gambling sites are not available to users in the United States. This is a popular method for darknet drug vendors to launder their proceeds and so those based in the U.S. will often access these online casinos by using VPN IP addresses that resolve to a nation allowed to participate in those particular online casinos.
  - vi. Eighteen deposits into VILLASENOR's Binance account received between February 6, 2021, and March 18, 2021, worth 3.68 BTC, were determined through tracing conducted by investigators to have sent from addresses associated with illicit DNM activity.
- c. Crypto.com –
- i. Crypto.com is a Singapore-based cryptocurrency exchange company. Users of this service commonly deposit fiat currency to be converted or traded via send/receive functions within the account application.
  - ii. A Crypto.com account under the name of Javier A VILLASENOR-Medina was identified pursuant to information received from a subpoena sent to Crypto.com,

based on blockchain tracing of transactions made by the Binance account controlled by VILLASENOR.

- iii. Of the 34 BTC deposits into this account, 20 of these deposits were sent from cryptocurrency addresses known to be associated with illicit DNM activities. Eight of the 34 deposits were ultimately from online gambling websites frequently used to launder illicit revenues. Overall, these deposits from known illicit or likely illicit sources accounted for 4.564 BTC of the total 5.07 BTC deposited into Crypto.com account 551937.
- iv. The Crypto.com cryptocurrency account remains active and has a balance that VILLASENOR regularly adds to and draws from.

49. Each of VILLASENOR's cryptocurrency exchange accounts transferred cryptocurrency between each other, with the balances from the now-dormant Coinbase and Binance accounts ultimately deposited into the Crypto.com account. Each of these accounts also received deposits that originated from blockchain addresses known to be associated with illicit darkweb activity. The addresses identified as associated with illicit DNM activities through tracing and previous investigations were from multiple address clusters. These addresses are identified below and were previously identified as an unknown blockchain service used for deposits sourced from "DarkMarket" and other DNMs in prior investigations.



- a. An unattributed service cluster consisting of 674 addresses associated with address 16WKZ\*\*\*. This address cluster has received cryptocurrency worth over one million USD from multiple DNMs, including “Empire Market” and “DarkMarket”.
- b. An unattributed service cluster consisting of 179 addresses associated with address 3G9Fj\*\*\*. This address cluster has received cryptocurrency worth over \$1.5 million USD from mixers and multiple DNMs, including “Hydra Market” and “DarkMarket”.
- c. An unattributed service cluster consisting of 767 addresses associated with address 1EXfo\*\*\*. This address cluster has received cryptocurrency worth over \$1.1 million USD from crypto currency mixers and multiple DNMs, including “Hydra Market” and “Icarus Market”.
- d. An unattributed service cluster consisting of 87 addresses associated with 14Jo9\*\*\*. This address cluster has received cryptocurrency worth over \$220,000 USD from multiple DNMs, including “Dark Market”.

50. On August 24, 2021, VILLASENOR purchased the Subject Vehicle from an identified subject in Tucson (this subject is not known to be involved in any illicit activity and appears unrelated to VILLASENOR beyond this vehicle sale). A corresponding outgoing transaction was identified in the information obtained from the subpoena returns

for Crypto.com account 551937 and 82,500 U.S. Dollar Coin (USDC)<sup>9</sup> was withdrawn from this Crypto.com account and sent to 0xF0C\*\*\* in Transaction Hash (TX) 0x9b3\*\*\*. This USDC balance was then sent to a new Crypto.com address (this is a separate address from the one associated with VILLASENOR's 551937 Crypto.com account) that was confirmed through subpoena returns to belong to the identified subject that sold the Subject Vehicle to VILLASENOR. VILLASENOR sent the Subject Vehicle to a Tucson-based high-end automotive upgrade business to have work done on the vehicle. The balance was partially paid using the Crypto.com credit card associated with account 551937 through two transactions, one for \$10,000 USD on September 9, 2021, and another for \$5,000 USD on September 15, 2021. There is probable cause to believe VILLASENOR used proceeds of his mail fraud involving the shipment of counterfeit or misbranded pills in interstate commerce that he falsely advertised and falsely sold as generic Xanax pills, to purchase and upgrade the Subject Vehicle. Further, there is probable cause to believe that the Subject Vehicle constitutes property involved in money laundering in excess of \$10,000.00.

51. According to Arizona DES (Department of Economic Security) records, VILLASENOR's reported employment income in 2018 was \$13,707. In 2019, his reported employment income was \$18,273 and in 2020 and 2021 his reported employment income was \$0.00. VILLASENOR during this time period was receiving approximately \$800.00 a week from his father's construction company into one of his primary checking accounts

---

<sup>9</sup> U.S. Dollar Coin (USDC) is a digital stable coin that is pegged to the United States Dollar.

separate and apart from his cryptocurrency accounts during 2020 and 2021 and none of that purported income appeared on DES records. VILLASENOR was never observed working at construction sites while under surveillance. And while there was activity observed by a pole camera of individuals working on their own cars at the warehouse location he rented, the activity resembled an auto club and not a business. Many times when VILLASENOR would show up at the warehouse, the others present would leave and VILLASENOR would be observed later exiting with packages in his possession.

### **Conclusion**

52. 21 U.S.C. § 853(f) specifically provides that a court may issue a criminal seizure warrant when it “determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that a [protective] order under [21 U.S.C. § 853(e)] may not be sufficient to assure the availability of the property for forfeiture.” An order under 21 U.S.C. § 853(e) may not be sufficient to ensure the availability of the Subject Vehicle for forfeiture because there is a substantial risk that it will be moved, sold or otherwise become unavailable unless immediate steps are taken to secure it at the time the requested seizure is executed.

53. Your Affiant believes that the facts contained herein demonstrate that there is probable cause to believe that the Subject Vehicle, a 2014 Nissan GTR 2 door coupe, VIN JN1AR5EF4EM270940, was purchased with proceeds derived from mail fraud in violation of 18 U.S.C. § 1341, and constitutes property involved in money laundering, in violation of 18 U.S.C. §§ 1956 and 1957, and is therefore subject to seizure pursuant to 18

22-07256MB

U.S.C. § 981(b), 21 U.S.C. § 881(b), and 21 U.S.C. § 853(f), and forfeitable pursuant to 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C), 982(a)(1), and 28 U.S.C. § 2461.

I declare under penalty that the foregoing is true and correct to the best of my knowledge, information and belief.

FURTHER, your affiant sayeth not.

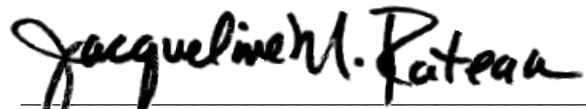
CONAN C  
BEACH

Digitally signed by CONAN C  
BEACH  
Date: 2022.05.09 16:01:18  
-07'00'

---

Conan Beach, Special Agent  
Homeland Security Investigations

Subscribed and sworn to telephonically this  
9th of May, 2022.



---

Jacqueline M. Rateau  
United States Magistrate Judge